REMARKS

The following is intended as a full and complete response to the Final Office Action dated September 1, 2010, having a shortened statutory period for response set to expire on December 1, 2010. By virtue of this amendment, no claims are amended, canceled or added. Claims 1-20 were examined and remain pending. The Examiner rejected claims 1-20 under 35 U.S.C. § 102(e) as being anticipated by Chen (U.S. Publication No. 2002/0076050). Applicants respectfully request reconsideration and withdrawal of these rejections for the reasons discussed below.

§ *102 Rejection of the Claims*

Claim 1 recites that "each of entitlement control messages [ECMs] is linked to a respective time-stamp, the respective time stamp associated with a time-stamp value indicative of a time at which the [ECM] linked to the time-stamp was distributed." Claim 1 further recites

> sending an entitlement management message [EMM] to a secure device, the [EMM] including a specification of a range of time-stamp values and entitling the secure device to enable decryption of the units of information that are linked to time-stamps with time stamp values in that range,
>
> wherein:
>
> the range has a starting point . . . prior to a time value corresponding to when the [EMM] is sent; and
>
> the starting point advances with the time value corresponding to when the EMM is sent.

Chen does not teach or suggest these limitations.

Chen discloses a system for securely delivering encrypted content on demand with access control. As summarized in paragraph 13 of Chen, unlike related art systems that employ real time encryption, the proposed system of Chen allows encrypting content offline before it is distributed to point-to-point systems, such as cable systems, and before the content is even requested by the subscriber. Such a system allows content to be encrypted only once, at a

centralized facility, and to be useable at different point-to-point systems. The system periodically performs an operation called ECM retrofitting enabling the pre-encrypted content to be useable in multiple systems and at multiple times in the same environment. In other words, ECM retrofitting allows the pre-encrypted contents in the system of Chen to have indefinite lifetimes (see paragraph 42 of Chen).

Figure 1 of Chen illustrates exemplary system 100 for delivering encrypted content to a subscriber. As explained in paragraph 46 of Chen, the system 100 includes a content preparation system (CPS) 102 for pre-encrypting content, a video on demand (VOD) system 108 storing encrypted programs for distributing to subscribers on an "on-demand" basis, conditional access system (CAS) 110 for controlling one or more keys granting access to pre-encrypted content, an encryption renewal system (ERS) 104 accepting requests from the VOD system to generate new ECMs for pre-encrypted content, a distribution network 112 for distributing content, and an interactive network 114 for providing two-way interaction between the subscriber and the content system.

The system 100 of Chen operates as follows. As described in paragraph 47 of Chen, once the VOD system is installed and properly registered with the ERS, content may be added to the VOD system and to be made available to subscribers. Clear content, such as a movie, originates from a content provider and begins its entry to the VOD at CPS 102, where the clear content is encrypted using an Off Line Encryption System (OLES). The OLES also generates an encryption record associated with the pre-encrypted content, where the encryption record includes the cryptographic keys or the parameters used in their generation (see paragraph 52 of Chen). Paragraph 48 of Chen proceeds to describe that the resulting pre-encrypted content and the associated encryption record are then delivered to the VOD system for storage on the local server. Paragraph 48 further discloses that, before the pre-encrypted content may be requested or viewed by subscribers in their homes, the VOD system obtains suitable ECMs from the ERS by, first, submitting an ECM request to the ERS, where the request contains the encryption record for the desired pre-encrypted content. Based on the encryption record, the ERS is able to generate one or more ECMs for the desired pre-encrypted content using the periodical cryptographic key associated with the cable system and possibly other parameters required by the CAS (see paragraph 66 of Chen). Therefore, next, the ERS responds with the proper ECMs,

an ERS synchronization number, and a callback time (see paragraph 49 of Chen). As described in paragraph 49 of Chen, the ECMs are created specifically for the particular pre-encrypted content and particular point-to-point system within which the VOD system operates, and for a particular time period. The ECMs encrypt content using a cryptographic key (typically periodical) provided to the ERS by each CAS controlling the set-top boxes (also see paragraph 43 of Chen). The VOD system then inserts the received ECMs into the streams along with the pre-encrypted content whenever it is distributed to a subscriber.

Paragraph 50 of Chen further elaborates that ECMs returned to the VOD system by the ERS are valid and usable with the pre-encrypted content only for a limited time. Namely, they are valid only until the callback time, where the callback time returned with the ECMs indicates the time by which the VOD system should check with the ERS to see if ECMs for all pre-encrypted content may be updated. In this manner, the ECMs may be created so that they will be valid until the periodical cryptographic key of the target system changes again (see paragraph 66 of Chen).

When the VOD system receives the callback time associated with the received ECMs for the desired pre-encrypted content, it stores the callback time and tracks it against the current time. When the current time reaches the callback time and the VOD system has not contacted ERS in the intervening time, the VOD system is configured to attempt to contact the ERS even if it has no new ECM requests to fulfill.

The Examiner argues that Chen's discussion of the periodical keys in paragraph 43, further discussion of the "particular time period" for which ECM is valid in paragraph 49, and the discussion of the "limited time" during which the ECM is "valid and useable" in paragraph 50 anticipates Applicant's "the range has a starting point kept at a predetermined distance prior to a time value corresponding to when EMM is sent" recited in claim 1, insofar as the periodical keys include a particular time period (range) during which the keys can be used to decrypt content. Applicant respectfully disagrees with such an interpretation of Chen and of the limitations of claim 1 for the following reasons.

First of all, claim 1 specifically recites that the "starting point of the range [is] prior to the time value corresponding to when an EMM is sent." Even if Chen could be interpreted as disclosing sending an EMM with a range of time-stamp values (which, by the way, would be an

incorrect interpretation, as discussed below), then, in contrast to claim 1, Chen could be interpreted as only specifying an ending point of the range, namely the "callback time." As described above, the callback time is some time in the future which "indicates the time by which the VOD system 108 should check with the ERS to see if ECMs for all pre-encrypted content may be updated" (see again paragraph 50 of Chen). In other words, the callback time disclosed in Chen is the time ***after*** the time when the message is sent. Therefore, Chen does not and cannot teach the limitation of "the range [having] ***a starting point . . . prior*** to a time value corresponding to when the [EMM] is sent," recited in claim 1 (emphasis added).

Second, Applicant believes that Chen also fails to disclose the limitation of "each of the [ECMs being] linked to a respective time-stamp, the respective time stamp associated with a time-stamp value indicative of a time at which the [ECM] linked to the time-stamp was distributed," recited in claim 1. As the foregoing description of Chen illustrates, the only element in Chen that could be considered in any way analogous to a "time-stamp linked to the [ECM]" recited in claim 1 is the "callback time." Again, as described above, this "callback time" disclosed in Chen is some time ***in the future***, some time after the time when the retrofit ECM was created (and/or distributed to the VOD system). By contrast, claim 1 recites that the time-stamp linked to the ECM is "indicative of the time at which the ECM ***was distributed***" (emphasis added).

Further, Applicant believes that Chen fails to disclose the limitation of "sending an [EMM] to [a] secure device, the EMM including a specification of [the] range of time-stamp values," as recited in claim 1. If the Examiner considers that the "range of time-stamp values," recited in claim 1, is analogous to the "limited time" during which the ECMs are "valid and usable" disclosed in Chen (see page 2 of the current Office Action), then first of all, according to Chen, such a range would be included in an ECM, not in an EMM, as recited in claim 1. Chen actually has a detailed description of what EMMs are and what ECMs are in paragraphs 4 and 5, respectively. Chen's description is consistent with the use of these terms in the present application (see, e.g., page 1, lines 6-21 and page 6, lines 1-10, of the application as filed) and makes clear that ECMs are different from EMMs. Second of all, according to Chen, a message including a specification of the range is sent from the ERS to the VOD system (see again, e.g., paragraph 49 of Chen and the description of Chen provided above) and not to the secure device

capable of selectively enabling decryption of units of encrypted information, as recited in claim 1. The VOD system disclosed in Chen may then communicate with the secure devices by sending ECMs and EMMs to the secure devices of the individual subscribers in a manner known in the art; however, there is no teaching in Chen that these messages from the VOD system to the secure devices would include any ranges of times such as, e.g., the range ending with the callback time. There is no such teaching in Chen because, as the above description of Chen illustrates, the callback time is only used by the VOD system to make sure that the ECMs which are included in a stream together with the encrypted content provided to the secure device of the subscriber are valid and useable at the time that the subscriber demands access to the content. Therefore, Chen does not disclose the limitation of "sending an [EMM] to [a] secure device, the [EMM] including a specification of [the] range of time-stamp values," recited in claim 1.

Finally, Chen fails to disclose the limitation of the "starting point [of the range advancing] with the time value corresponding to when the [EMM] is sent," recited in claim 1. As the foregoing illustrates, Applicant does not believe that Chen discloses the starting point of a range. At most, Chen may be considered to teach the ending point of the range, but even then, there is simply no teaching in the entire reference that this point would be advancing with the time value. In fact, Chen teaches away from it because knowing that this point advances with the time value of when EMM is sent would make the time limit predictable in advance. But Chen teaches, in paragraph 50, that the exact time during which the ECMs returned to the VOD system are valid and useable is determined by the CAS and is "not predictable in advance."

In conclusion, the system described in Chen fails to disclose most of the limitations of claim 1 because the system disclosed in Chen is designed to allow the secure device of the subscriber to decrypt live encrypted content, while the method and system of the present invention intend to enable access to stored encrypted content (see, e.g., page 2, lines 21-27, of the application as filed).

As the foregoing illustrates, the limitations of "each of [ECMs] [being] linked to a respective time-stamp, the respective time stamp associated with a time-stamp value indicative of a time at which the [ECM] linked to the time-stamp was distributed" and the limitations of

> sending an [EMM] to [a] secure device, the [EMM] including a specification of a range of time-stamp values and entitling the

> secure device to enable decryption of units of information that are linked to time-stamps with time stamp values in that range,
>
> wherein:
>
> the range has a starting point . . . prior to a time value corresponding to when the [EMM] is sent; and
>
> the starting point advances with the time value corresponding to when the [EMM] is sent

are not taught in Chen. For this reason, Applicant submits that claim 1 is in condition for allowance and requests that the 102 rejection be withdrawn.

Independent claims 7, 9, 10, and 20 recite limitations similar to those of claim 1. Therefore, these claims are in condition for allowance for the same reasons. Claims 2-6, 8, and 11-19 are dependent from allowable claims 1, 7, and 10, and, therefore, are also in condition for allowance.

Reservation of Rights

In the interest of clarity and brevity, Applicant may not have equally addressed every assertion made in the Office Action, however, this does not constitute any admission or acquiescence. Applicant reserves all rights not exercised in connection with this response, such as the right to challenge or rebut any tacit or explicit characterization of any reference or of any of the present claims, the right to challenge or rebut any asserted factual or legal basis of any of the rejections, the right to swear behind any cited reference such as provided under 37 C.F.R. § 1.131 or otherwise, or the right to assert co-ownership of any cited reference. Applicant does not admit that any of the cited references or any other references of record are relevant to the present claims, or that they constitute prior art. To the extent that any rejection or assertion is based upon the Examiner's personal knowledge, rather than any objective evidence of record as manifested by a cited prior art reference, Applicant timely objects to such reliance on Official Notice, and reserves all rights to request that the Examiner provide a reference or affidavit in support of such assertion, as required by MPEP § 2144.03. Applicant reserves all rights to pursue any cancelled claims in a subsequent patent application claiming the benefit of priority of

the present patent application, and to request rejoinder of any withdrawn claim, as required by MPEP § 821.04.

CONCLUSION

Based on the above remarks, Applicants believe that they have overcome all of the rejections set forth in the Final Office Action dated September 1, 2010, having a shortened statutory period for response set to expire on December 1, 2010, and respectfully submits that the claims are in condition for allowance, and notification to that effect is earnestly requested. The Examiner is invited to telephone the undersigned at (408) 278-4051 to facilitate prosecution of this application.

If necessary, please charge any additional fees or deficiencies, or credit any overpayments to Deposit Account No. 19-0743.

Respectfully submitted,

SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. Box 2938
Minneapolis, MN 55402--0938
(408) 278-4051

Date 10/28/2010

By /Karen Kaufman/
Karen L. Kaufman
Reg. No. 57,239